UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/542,904	07/20/2005	Johan Paul Linnartz	NL 030088	1783

24737 7590 10/27/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2431	

MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/542,904	**Applicant(s)** LINNARTZ, JOHAN PAUL MARIE GERARD	
	Examiner LONGBIT CHAI	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Currently pending claims are 1 – 10.

Response to Arguments

2. Applicant's arguments filed on 9/24/2008 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn and, upon further consideration, a new ground of 35 U.S.C. 102(e) rejection has been made – see the following Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 – 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Lotspiech et al. (U.S. Patent 6,888,944), hereafter referred to as Lotspiech-944 with "incorporated by reference" of Lotspiech et al. (U.S. Patent 6,118,873), hereafter referred to as Lotspiech-873).

As per claim 1, 8 and 9, Lotspiech teaches **a method of granting access to content on a storage medium** (Lotspiech-944: Column 1 Line 20 – 22) & (Lotspiech-9873: Column 1 Line 13 – 21: a set-top box as a data storage medium), comprising:

obtaining cryptographic data from a property of the storage medium (Lotspiech-944: Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: the index (codeword) of the last define set of key is qualified as the cryptographic data, which is stored at a property of a data storage device);

reading helper data from the storage medium (Lotspiech-944: Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: the redundant bits portion associated with the Generating Matrix [G] used by typical error-correcting code technique related to hamming distance is qualified as the helper data – This is also consistent with the disclosure of the specification of the instant application (SPEC: Page 11 Line 15 – 16: the redundancy bits are taken directly from the helper data).

granting the access based on an application of a delta-contracting function to the cryptographic data and the helper data (Lotspiech-944: Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: using typical "error-correcting code" technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored (a) compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function and (b) access to content data is granted implicitly with correctly generated decryption key so that the encrypted content can be decrypted correctly and otherwise, decryption would fail and no proper output can be obtained (i.e. access is denied) if the generated decryption key is incorrect (Lotspiech-944: Column 3 Line 8 – 9)).

As per claim 2, Lotspiech teaches deriving a decryption key for decrypting the content at least from the application of the delta-contracting function (Lotspiech-944: Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: using typical "error-correcting code" technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function).

As per claim 3, Lotspiech teaches deriving a decryption key further derives the decryption key from data supplied by a playback or recording apparatus (Lotspiech-944: Column 4 Line 58 – 62: device serial number).

As per claim 4, Lotspiech teaches the access is granted if the output of the delta-contracting function corresponds to a control value recorded on the storage medium (Lotspiech - 944: Column 4 Line 49 – 57 / Column 7 Line 7 – 13; Lotspiech–873: Column 6 Line 30 – 37 and Column 2 Line 10 – 14: (a) the output of the delta-contracting function, as taught by Lotspiech-944, that generates a set of device keys are used to decrypt the encrypted session secret numbers and all of the decrypted session secret numbers are then hashed to produce a content session key so that the digital content can be successfully decrypted, as taught by Lotspiech-873 and as such, Examiner note the output of the delta-contracting function (i.e. the derived device key) must be corresponding to a set of stored "session secret numbers" (i.e. a control value recorded on the storage medium) so that a valid content session key can be obtained and, as a result, the valid digital content can then be granted for authorized access).

As per claim 5, Lotspiech teaches applying a cryptographic function to the output of the delta-contracting function and comparing the output of the cryptographic function to the control value (Lotspiech–944: Column 4 Line 49 – 57 / Column 7 Line 7 – 13; Lotspiech–873: Column

6 Line 30 – 37 and Column 2 Line 10 – 14: (a) The output of the delta-contracting function, as taught by Lotspiech–944, that generates a set of device keys are used to decrypt the encrypted session secret numbers and all of the decrypted session secret numbers are then hashed to produce a content session key, as taught by Lotspiech–873 and as such Examiner notes a hash function is qualified as a cryptographic function to meet the claim language).

As per claim 6, Lotspiech teaches the cryptographic function is a one-way hash function (see the same rationale of rejection on claim 5: a one-way hash function).

As per claim 7, Lotspiech teaches the delta-contracting function involves a combination of a matrix multiplication on the cryptographic data, a linear addition of at least a portion of the helper data, a quantization in which the quantization areas are defined by a portion of the helper data, and error correction decoding (Lotspiech-944: Column 2 Line 26 – 33, Column 4 Line 49 – 57 / Column 7 Line 7 – 13 and Column 3 Line 7 – 9: using typical "error-correcting code" technique to generate sets of encryption key for a player-recorder apparatus with hamming distance between two sets of keys, where the stored (a) compact generating function characterized by Generating Matrix [G] is qualified as a delta-contracting function, (b) the index of the last define set of key is qualified as the cryptographic data, and (c) the redundant bits portion associated with the Generating Matrix [G] used by typical error-correcting code technique related to hamming distance is qualified as the helper data – This is also consistent with the disclosure of the specification of the instant application (SPEC: Page 11 Line 15 – 16: the redundancy bits are taken directly from the helper data); which is also qualified as a quantization in which the quantization areas related to the hamming distance associated "quantization tolerance").

As per claim 10, Lotspiech teaches a computer program product arranged to cause a processor to execute the method of claim (Lotspiech-944 : Column 2 Line 19 – 22).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D
Primary Examiner, Art Unit 2431
10/14/2008